DISA IAVA PROCESS HANDBOOK

Version 2.1

11 June 2002

1.0 Introduction

The Department of Defense (DOD) is concerned with threats, both potential and real, to their information systems and networks. We live in an era where dependencies on information systems supporting the warfighter are more critical than ever before and the assets that comprise these information systems must be protected through risk management. To provide the proper framework to accommodate any deliberate or unintentional attempt at exploiting DOD information the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD/C3I) tasked a process to be developed that will fulfill the following requirements:

1) Establish positive control of the Department's vulnerability alert system.
2) Provide Commanders-in-Chief (CINC), Services, and Agencies (C/S/As) access to vulnerability notifications that require action.
3) Require acknowledgement of action messages.
4) Require compliance and report status to DOD (DISA).
5) Track compliance and report to OSD.
6) Conduct random compliance checks.

The process identified to fulfill these requirements is titled the Information Assurance Vulnerability Alert (IAVA) process. This process is designed to provide a measure of risk avoidance within the overall risk management framework.

DISA has two distinct IAVA responsibilities. The first responsibility is as the DOD agent in charge of managing vulnerability notices. The second responsibility is as an agency implementing and managing vulnerability notices and reporting statistics to the IAVA Web site. This document relates to the responsibilities associated with DISA/National Communications System (NCS) acting as an agency in managing vulnerability notices. The DISA IAVA process is a part of the DISA overall vulnerability management (VM).

To be successful within DISA, the process must incorporate or be incorporated into configuration management processes. The IAVA process is intended to provide a means of obtaining positive control down to the system asset level. The information to be reported via the IAVA process consists of the numbers of systems on which the vulnerability exists, when compliance has been achieved, when an extension has been requested, and when an extension has been granted.

1.1 Purpose of the IAVA Process Handbook

This handbook, developed by the DISA Chief Information Officer (CIO), provides a single point of reference on how DISA will implement and maintain a proactive IAVA process. The handbook will also provide guidance on what DISA activities and major programs need to know to implement and manage the IAVA process in support of their missions. The process relies on two distinct tools: 1) the IAVA system, and 2) the Vulnerability Compliance Tracking System (VCTS). The IAVA system is a database used to track compliance statistics at the C/S/A level. The VCTS is a database system that is used to track the status of vulnerabilities at the asset level. The VCTS statistics are rolled up to the IAVA system for a compliance view within the agency. Further information on both of these tools is provided throughout this document.

1.2 Handbook Applicability

This handbook is applicable to the most current version of VCTS. As updates occur with the process and tools, this handbook will be updated accordingly.

1.3 Handbook Organization

Revisions made from v.2.0 to v.2.1 highlighted on pages: 4, 5, 6, 9, and Annex E.

This handbook is organized to help the reader understand various pieces of the DISA IAVA process. The following summarizes the content of each section within the handbook.

Section 1 – Introduces the handbook and describes the overall purpose of the handbook.

Section 2 – Provides an overview of the actual IAVA process. This includes information on how vulnerability notices are generated, the responsibilities of C/S/A in managing vulnerability notices, as well as the methodology DISA uses in managing vulnerability notices.

Section 3 – Outlines the applicable references associated with the IAVA and VCTS processes.

Section 4 – Provides a high-level overview of the VCTS process and introduces key terms such as assets and compliance status.

Section 5 – Contains the detailed information on the processes within VCTS. The information is organized from the perspective of the user category (e.g.; Systems Administrators (SA), Information Systems Security Manager (ISSM)).

Section 6 – Outlines the compliance validation process and how it currently works within DISA.

Section 7 – Contains information on other uses for VCTS.

Section 8 – Documents the points of contact for the various elements of the process.

Annex A – Provides a glossary of terms used throughout the handbook.

Annex B – Contains the table of contents for VCTS online Users Guide.

Annex C – Contains a sample VCTS IAVA Alert message.

Annex D – Addresses general questions and answers.

Annex E – Fix Action Plan format.

2.0 IAVA process Overview

This section provides an overview of the IAVA process and discusses the development of a vulnerability notice, along with the responsibilities for each C/S/A in managing vulnerability notices. The information in this section is applicable to every C/S/A.

2.1 IAVA Development

The IAVA process begins with vulnerabilities being identified by or reported to DISA. The DISA DOD-Computer Emergency Response Team (DOD-CERT) researches the vulnerability to determine the impact, severity, and means of correcting or mitigating the risk associated with the vulnerability. If the results of this analysis indicate a need for action, the DOD-CERT will perform one of the following actions:

1) Issue an Information Assurance Vulnerability Alert (IAVA) - requires acknowledgement and compliance,
2) Issue an Information Assurance Vulnerability Bulletin (IAVB) - requires acknowledgment only, or
3) Issue a Technical Advisory (TA) - notification only.

Once the VULNERABILITY NOTICE has been developed, the DOD-CERT notifies each C/S/A's point of contact, via approved communication channels, that an alert, bulletin, or technical advisory has been issued and that the details can be accessed at the DOD-CERT NIPRNET Web page (WWW.CERT.MIL) or on the SIPRNET (WWW.CERT.SMIL.MIL).

2.2 IAVA - CINC/Service/Agency (C/S/A) Responsibilities

Each C/S/A, upon receipt of an official notification of a vulnerability notice, has several responsibilities. DISA, as a defense agency, must take the appropriate actions for the vulnerability notice. A high-level view of the responsibilities is outlined below.

First, access the DOD-CERT Web Page and retrieve the entire vulnerability notice message.

Second, notify SA, ISSO, and all appropriate staff of the vulnerability notice and inform the staff to access the DOD-CERT Web Page and retrieve the vulnerability notice message.

Third, acknowledge receipt of the vulnerability notice notification to the DOD IAVA Web site. Acknowledgement must be completed within 5 days unless otherwise specified in the vulnerability notification.

Fourth, assess the impact of the vulnerability, apply the fix or obtain an extension if corrective actions cannot be implemented within the specified timeframe. Report the status for each vulnerability notice as it applies to every applicable asset within its area of responsibility.

Each C/S/A's official response is via the DOD IAVA Web site within 30 days from issuance of the vulnerability notice unless otherwise specified in the vulnerability notice. If an extension is granted by a C/S/A designated Approving Authority (DAA), the following considerations must be documented:

- The assessment of risk (e.g.; how vulnerable the environment is to the exploit)
- How the system(s) will be monitored for exploitation (e.g.; use of mitigating controls)
- A Fix Action Plan with a completion date

Fifth, conduct random compliance checks on assets to validate the information being reported through the command channels.

2.3 DISA's IAVA Implementation

DISA, as a DOD agency, is responsible for implementing the guidance internally, as well as having overall responsibility for the IAVA process throughout DOD. To support DISA's internal implementation of the IAVA process, DISA has developed a tool called the Vulnerability Compliance Tracking System (VCTS). The VCTS is used to track compliance information for each DISA organization at the asset level.

DISA can opt to make a vulnerability notice requirement more stringent than those required by the DOD CERT. DISA requires this for compliance with IAVBs or acknowledgement for technical advisories (TA). This is accomplished through the VCTS notice process.

3.0 References

Several references have been published on IAVA and VCTS tools and processes. This section lists all of the applicable references.

1) DoD CERT references available at DoD CERT website at URL http://www.cert.mil/iava/iava_index.htm.
   Mandates the implementation of the IAVA process throughout the DOD community.

2) Vulnerability Compliance Tracking System User's Guide.
   Provides additional information on the actual usage of VCTS.

3) DISAI 630-230-19, Information Systems Security Program, 09 July 1996.
   Documents DISA policy in regard to general IA issues.

4.0 VCTS Overview

The Vulnerability Compliance Tracking System (VCTS) is a Web-based DoD application used to assist DISA in managing its internal implementation of the IAVA process. The VCTS currently allows vulnerability compliance information for individual system assets to be managed by the SA, and monitored by the ISSM and/or Executive Officer (XO) or appropriate PM's (i.e. Defense Message System (DMS), Global Command and Control System (GCCS), etc.).

The compliance information for the assets within VCTS are then summarized and uploaded to the IAVA Web-based application. This ensures that the DISA statistics reported to the ASD/C3I or the Joint Staff are current and that progress can be monitored on a regular basis. See *paragraph 4.3* for the VCTS process flow.

4.1 VCTS Systems

DISA maintains two VCTS systems: one for unclassified assets and one for classified assets. All DISA information technology (IT) assets that are susceptible to vulnerabilities shall be registered in the VCTS.

All DISA IAVA information for ***unclassified*** assets is stored on the ***unclassified*** VCTS database. All information entered and stored into this database is considered Sensitive But Unclassified (SBU) and is protected accordingly.

All DISA IAVA information for ***classified*** assets is stored on the ***classified*** VCTS database. All information entered and stored into this database is considered no higher than Secret and is protected accordingly.

4.2 VCTS Tracked Assets

All IT assets (sometimes called system assets) that are susceptible to vulnerabilities must be registered in the VCTS. In general, individual workstations will not be registered in VCTS. Instead, the server(s) will be registered and the appropriate field completed showing the number of workstations it supports. However, individual machines not managed by a server environment must be registered to ensure proper tracking of vulnerability alerts.

Each asset, to include mirrored assets, must be registered. It is acknowledged there are mirrored installations. However, due to phased implementations and tendencies to change, it is required that each asset be registered accordingly.

There may be instances where systems do not need to be registered in VCTS. An example could be a GOTS developed product that does not rely on functions typically available in commercial products. If it is felt that the asset does not require VCTS registration, a letter must be submitted by the Principal Director, Director, or Commander for the organization to the DAA requesting a exemption of VCTS registration. The DAA will then evaluate the request and inform the site of the decision.

Laptop computers, network printers, facsimiles, and all personal electronic devices (PED's) are not required to be registered in the VCTS at this time. However, DISA activities are encouraged to register the operating system (OS) of like laptops. Each activity will then monitor the assets for vulnerabilities associated with the laptops OS.

Assets within VCTS are generally defined in four categories: organizational assets, program level assets, mainframe assets and laboratory assets. Additional information on these assets is covered in the following paragraphs.

4.2.1 Organizational Assets

Organizational assets are those that a site is responsible for and does not rely on a program management office for guidance and support. The site operating the system registers these assets and the site makes decisions regarding vulnerability notices.

4.2.2 Program Managed Assets

Program level assets are those that a program office provides guidance. The process for registering and maintaining compliance status for these systems depends upon the program. In some cases, such as DISANet, the DISANet program office registers the systems and manages the implementation of corrective actions. In other programs, the site is responsible for registering these assets, but the program office analyzes the vulnerability notice and provides details regarding corrective actions to be taken. Information must be obtained through each program office to determine how these assets are to be managed. All DISA PMs are encouraged to use the capabilities developed for them within the VCTS. (Contact cioiase@ncr.disa.mil for details.)

4.2.3 Mainframe Assets

Since the mainframe systems (e.g. MVS, UNISYS, TANDEM) run services such as TCP/IP and the UNIX kernel, mainframe systems must be registered in VCTS. Each logical domain/image must be registered. The system ID field should be populated with an IP address.

Because a mainframe system typically has a staff of systems programmers responsible for the software configuration, registration of mainframe assets will be managed by the ISSO. Throughout this document, the term system administrator will include the ISSO as it relates to asset management in VCTS.

4.2.4 Laboratory Assets

All assets permanent, temporary or transitional that are attached to a network outside of the laboratory will be registered in the VCTS.

In some cases within DISA, devices/assets are acquired from a vendor to perform testing in a laboratory environment. Laboratory assets are acknowledged as unique because of each laboratory's mission. Laboratory assets will be identified and tracked using the following guidance:

1) **Permanent laboratory asset** is any IT asset residing in a laboratory without any major configuration change within 120 consecutive calendar days. These assets will be registered in the VCTS. These assets will maintain IAVA compliance.

2) **Temporary or Transitional laboratory asset** is any IT asset residing in a laboratory with major configuration changes within 120 consecutive calendar days. Recommend these assets be registered in the VCTS, but it's not mandatory. It is recommended that these assets maintain IAVA compliance. However, the laboratory lead SA is responsible for using good judgment in applying corrections as issued in the alerts.

A lead SA will be appointed for each laboratory and the lead SA will receive all vulnerability notices issued. Each lead SA must have at least one backup SA. It is the lead SAs responsibility to:

1) Identify each type of laboratory asset (permanent or temporary/transitional),

2) Determine what assets will be registered in the VCTS,

3) Oversee IAVA compliance for the assets residing in the laboratory,

4) Ensure all assets leaving the laboratory for operational purposes are in IAVA compliance.

4.3 VCTS Process Flow

Once a vulnerability notice has been issued by the DOD-CERT, VCTS will send notices, via email, to the responsible SA(s) and ISSOs associated with the applicable assets. Notices also will be sent to all ISSMs and all XOs, for all vulnerability notices issued. The VCTS notice will direct the user to access the DOD-CERT Web site to obtain the detailed information for the specific vulnerability notice. An example of the emailed VCTS IAVA Notification message is shown in ***Annex C***.

At least one SA for each asset must acknowledge receipt. That individual is then responsible for initiating the process of evaluating and correcting the vulnerability. As the status of the vulnerability changes, each asset in VCTS must be updated with the current status. For example, the status may be that a fix was applied, an extension was requested, or that the vulnerability notice was not applicable to the component.

Further information regarding the IAVA Process flow can be found in the VCTS Users Guide.

4.4 Compliance Status

Every asset potentially affected by a vulnerability notice will be labeled with one of the following "Compliance Status" identifiers:

Open: As soon as an asset is entered into the VCTS, this asset is assigned an "open" status, until a decision is made otherwise by the individual who has custody for the asset. "Open" means the asset is impacted by a specific alert; however, no protective actions have been put in place. As a result, the vulnerability still exists. Most alerts are issued with a period of 30 days for compliance. An "open" status is acceptable during this 30-60 day period. However, if an asset becomes operational and is registered in the VCTS 30 days after the initial release of the alert, an "open" status is **not acceptable**.

Not Applicable: "Not applicable" means the SA, ISSO, ISSM or PM has determined a recently released alert does not apply to the operational configuration of a registered asset in the VCTS. The responsible user who made this decision is required to maintain all documentation to justify the "Not Applicable" status. The management hierarchy or the DAA may request the documentation. Also, the documentation may be reviewed during the IAVA compliance validation process.

Fixed/In Compliance: This status means the SA or ISSO has determined a registered asset is applicable to a recently released alert and is in compliance with the official patch or fix.

Extension Requested: "Extension Requested" indicates that an extension request has been submitted for this asset and is in the process of being reviewed. There are two types of extension requests. First, the extension can be used in the traditional sense where the DAA accepts the mitigated risk associated with nonstandard official corrective action. Second, the extension can be employed by the user to request additional time to allow for corrective action to occur. This would be used for situations where corrective actions cannot be implemented within the specified timeframe due to other factors (e.g.; equipment delivery, financial limitations, resource shortage, PMO actions, and other prerequisite tasks). Information regarding extension responsibilities for SAs can be found in Section 5.4 and for DAAs in Section 5.7.

Extension Approved: This status indicates that an extension request has been approved for a specified timeframe. Management is responsible for continuing to address the problem and ensure that mitigating controls are in place. An extension may be granted for extended periods with management involvement. See list below.

	Number of Days	Management	Fix Action Plan Requirement
Original IAVA Compliance Period	30 < original time period	ISSM	- Email tickler sent 15 days prior to compliance date polling activity fix status. - If asset will be in compliance – No action required. - If asset will not be in compliance – Each activity ISSM must submit a consolidated activity Fix Action Plan* to CIO 7 days prior to IAVA compliance date.
1st Extension	Not to exceed 30 days	ISSM, DAA	- Email tickler sent 15 days prior to compliance date polling activity fix status. - If asset will be in compliance – No action required. - If asset will not be in compliance – Each activity ISSM must submit a consolidated activity Fix Action Plan* to CIO 7 days prior to extension expiration.
2nd Extension	Not to exceed 60 days	ISSM, DD, DAA	- Email tickler sent at 15-day intervals for compliance status check.
Additional Extensions (if required)	Based on circumstances	DD, DAA, D, JCS	TBD

* Fix Action Plan format is included under Annex E.

Extension Denied: This status indicates that the Designated Approval Authority evaluated and denied an extension request. The SA/ISSO is responsible for immediately implementing corrective actions.

Extension Expired: This status indicates that an approved extension has expired for the asset and that corrective actions must be implemented or that another extension request must be submitted.

5.0 VCTS Process Details

This section contains the information on how to access and use the VCTS system from a process point of view. Detailed information on the fields and values within VCTS can be found in the VCTS User's Guide (accessible online through the VCTS Web page at https://vcts.disa.mil or email weblog@chamb.disa.mil).

5.1 Obtaining/Changing/Deleting Access to VCTS

To obtain access to VCTS, each individual user must have a unique userid and password. All initial, change, and delete requests for access to the VCTS must be requested by completing DISA Form 41, System Authorization Access Request (SAAR) which can be accessed using the DISA Standard FormFlow application. The following information is required:

Block 16 - Indication of VCTS System to be accessed (unclassified, classified, or both)

Block 18:

- IP Address of the Users workstation
- Subnet Mask Specified for the workstation
- Whether Dynamic Host Configuration Protocol (DHCP) is being used
- Internet Email address
- United States Postal Service (USPS) mailing address

Once the SAAR is completed, it should be forwarded to:

DECC-D Chambersburg
ATTN: Security
Letterkenny Army Depot, Building 3
Chambersburg, PA 17201-4186

FAX (717) 267-8264, DSN 570-8264.

Once RSA Chambersburg receives the SAAR, processing will occur within 5 working days. A userid and password will be mailed to the requester under separate cover letter. Included will be a password receipt form that must be signed and faxed back to RSA Chambersburg. Once the signed form has been received, the userid will be activated.

The process for changing or deleting a users access to VCTS is also accomplished through the use of Form 41. To ensure the integrity of the system and the data, it is required that users who no longer require access to VCTS be removed from the system. A user's access can be suspended by the ISSM through the RSA Chambersburg Help Desk. However, the ISSM is responsible for ensuring that Form 41s requesting removal of access are processed for users no longer requiring access. It is recommended that this procedure be incorporated into the checklist used for personnel actions such as transfers, resignations, or even Temporary Duty Assignments (TDY).

If the userid or password is forgotten, the RSA Chambersburg Help Desk can provide assistance in restoring access. If the password becomes compromised, the Helpdesk should be notified immediately to facilitate the appropriate actions.

DISA will perform an annual reconciliation of users to ensure accuracy of the users defined to VCTS.

5.2 Accessing VCTS

VCTS can be accessed using DISANet's standard browser requirements. However, the application does use SSL 128 bit key encryption. As a result, ensure that the product to be used has the correct encryption module installed. Further details can be obtained through either the VCTS Users Guide or through the RSA Chambersburg Help Desk.

The unclassified VCTS system can be accessed on the NIPRNET at https://vcts.disa.mil. The classified VCTS systems can be accessed on the SIPRNET at https://vcts.disa.smil.mil. Procedures for accessing VCTS can be found in the information mailed as part of the registration process and in the VCTS Users Guide.

5.3 VCTS Users Guide Table of Contents

Specific details on the use of VCTS can be found in the VCTS online Users Guide. A table of contents for VCTS can be found in Annex B.

5.4 SA/PM Extension Processing

The SA/PM is responsible for the generation of an extension request. This is accomplished by changing the status to "extension requested" and providing the supporting information in the Comment Text field. The information provided as part of the extension request must include the reason for the extension, the estimated completion date for fixing the vulnerability, documentation supporting a risk assessment, and a description of the mitigating controls being implemented to manage the vulnerability until the actual documented fix is implemented.

SAs need to follow these steps to assure that an extension is needed;

1. Once a vulnerability notice is issued, check if the vulnerability is applicable to the asset.
2. Check if any fixes/solutions are available.
3. Check if the asset is PM controlled or related.
4. Contact the activity ISSM for verification.
5. Develop a fix action plan.
6. Write a supporting paragraph to be placed in the "comments" field inside VCTS.

Once an extension request has been initiated, the responsibility for the request is forwarded to the DAA representative. Once the DAA has acted upon the request, the status of the asset is changed appropriately. The assets that have had the extension granted will have their status changed to "extension granted". At this point, the SA/PM has until the estimated completion date associated with the vulnerability notice/asset to come into compliance.

When an extension expires, the status of the vulnerability will change to "extension expired". This is considered as an open status. As a result, the SA/PM or ISSO must take immediate action to either fix and close the vulnerability, or request an additional extension. Any extension beyond the first must be approved by the DD or XO.

Those assets that have had the extension denied will have their status changed to "extension denied". At this point, it becomes the responsibility of the SA/PM to comply with the corrective actions immediately.

5.5 Information Systems Security Managers (ISSMs)

Information Systems Security Managers (ISSMs) are responsible for ensuring that the vulnerabilities for systems within their area of responsibility are being addressed by the SAs or ISSOs. An ISSM may be given “update” authority to a system but must follow the procedure outlined in the VCTS Users Guide.

An ISSM is responsible for:

1. Validate current user accounts and permissions and remove accounts not required (VM03 report) in the classified and unclassified VCTS databases.

    a. Run the VM03 report.
    b. Determine if there are active users who should no longer have access.
    c. Contact the assets primary SA for removal of unnecessary permissions.
    d. Request the user account be inactivated by sending an email to weblog@chamb.disa.mil with a list of users that should be deactivated or using a DISA Form 41 and checking the delete account block and faxing it to DSN 570-8264 or commercial (717) 267-8264.

2. Validation of current asset information (VM04 report) in the classified and unclassified VCTS databases.

    a. Run the VM04 report.
    b. Determine if the asset description information is accurate and current. Contact the assets primary SA for action.
    c. Asset SA should correct asset information as needed. (The SA who makes a change to an assets record in the VCTS will become the "NEW" Primary SA of record for that asset).

3. Ensure all ISSOs and Sac’s are familiar with the registration process.
4. Ensure each asset has at least two (2) users with update permissions.
5. Properly validate extension requests for the activities assets when needed.

Further information regarding the report capabilities can be found in the *VCTS Users Guide*.

5.6 Executive Officers (XOs)

Executive Officers (XOs) are responsible for ensuring that the vulnerabilities are being managed by the ISSMs. The XOs have overall responsibility to ensure that the information recorded within VCTS is accurate for their organizations. The XOs generally are not given authority to update systems, but rather, have browse authority to monitor the progress in complying with vulnerability notices. The authority to browse systems is implicit for their organization. An XO does not have to be given “browse” authority by the SA or ISSM for an asset.

Further information regarding the report capabilities can be found in the VCTS Users Guide.

5.7 Designated Approval Authority (DAA) Representative

DAA representatives have responsibility for the acceptance of risk for all assets within the agency and must approve or deny any requests for extension. The DAA can view all assets within the agency since they are ultimately responsible for the certification and accreditation of these assets. Today, DISA has divided the responsibility for accreditation between two organizations: Operations (OPS) for DISA managed DOD systems and CIO for DISA internal mission systems. The CIO Information Assurance Division (IAD) provides DISA accreditation support to both the OPS and CIO DAA's. Thus, the CIO IAD administers the VCTS approval process and coordinates with OPS as appropriate.

5.8 Extension Technical Analysis

When an SA initiates an extension request through the System Status screen, an extension number is assigned and the DAA representative is notified that an extension request needs to be analyzed.

The technical analysis of an extension consists of reviewing the risks associated with the vulnerability. Several pieces of information are reviewed in assessing an extension request. Examples of such information include, but are not limited to, the following:

- Reason for the extension request
- Input from the applicable PMO
- Mitigating controls being implemented
- Sensitivity of the information processed in the environment
- Severity of the vulnerability
- Likelihood of the vulnerability being exploited
- Estimated date of compliance with the fix

Once the DAA representative has reviewed the information, a decision is made and the result recorded within VCTS.

5.9 Extension Acceptance and Denial

Once a decision has been made regarding an extension request, the CIO updates the status in VCTS. The Estimated Completion Date Field is updated if necessary by the CIO to indicate the date that full compliance is expected to be achieved by. The CIO may also provide text that needs to be reviewed by the SA.

The assets that have had the extension granted will have their status changed to "extension granted". Those assets that have had the extension denied will have their status changed to "extension denied". At this point, it becomes the responsibility of the SA to correct the vulnerability associated with the asset and to comply with any comments provided by the CIO.

6.0 Vulnerability Notice Compliance Validation Process within DISA.

The IAVA process as directed by the Secretary of Defense requires a vulnerability notice Compliance Validation (CV) Process for each C/S/A (reference section 3.0; reference 1). DISA's IAVA CV Process is currently under development. In the interim, to ensure awareness and visibility throughout the agency, the CIO provides a weekly e-mail notices to each organization's ISSM and their Deputy Director to review and validate all their vulnerability notice entries in the VCTS. Each organization is responsible to ensure that all data in VCTS is accurate and current.

7.0 VCTS – Other Uses Within DISA

Periodically DISA management has a requirement for either collecting or disseminating information agency wide; i.e. identifying firewalls, intrusion detection systems, routers, etc. DOD may also task C/S/As to follow specific guidance and report back; i.e. Joint Task Force Tasking Orders. Management uses the VCTS as a tool to assist them in the collecting and disseminating for this type of information. The naming convention for this type effort is called the "DDIR" vice 'vulnerability notice'. The format for the DDIR is similar to the vulnerability notice in it uses a similar numbering convention; i.e. DDIR-yyyy-nnnn.

8.0 Points of Contact within DISA.

8.1 VCTS.

VCTS USERID and Password – DECC-D Chambersburg Helpdesk. VCTS help can be received at the DECC-D Chambersburg helpdesk or by sending an email to weblog. Application specific questions or suggestions can be sent to vms@chamb.disa.mil. The telephone number is (717) 267-5690, DSN 570-5690, 1-800-582-4764, or via the NIPRNET email at weblog@chamb.disa.mil.

VCTS System Developers – APPS. The systems development group can be reached via NIPRNET email at vms@chamb.disa.mil

VCTS Process Assistance – CIO. The telephone number is (703) 681-2558, DSN 761-2558, or via the NIPRNET email at cioiase@ncr.disa.mil.

Annex A – Acronyms and Abbreviations

ASD/C3I	Assistant Secretary of Defense – Command, Control, and Communications.
Asset	See “System Asset”
CIO	Chief Information Officer
Command Staff	Leaders of an organization responsible for ensuring compliance with the IAVA process
Compliance	Correcting the vulnerability in a vulnerability notice using the processes documented in the alert.
C/S/A	Commanders-in-Chief (CINC), Services, and Agencies
DAA	Designated Approving Authority
DISA	Defense Information Systems Agency
DOD-CERT	Department of Defense – Computer Emergency Response Team.
IAVA	Information Assurance Vulnerability Alert – A formal notice issued by the DOD-CERT requiring acknowledgment and compliance within a specified timeframe
IAVB	Information Assurance Vulnerability Bulletin – A formal notice issued by the DOD-CERT requiring acknowledgment only within a specified timeframe
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
SA	System Administrator
SSAA	System Security Authorization Agreement
System Assets	Any software, hardware, data, administrative, physical, communications, or personnel resources within an Information System (i.e. file servers, firewalls, routers, etc.) NSTISSI No. 4009 (Sep 2000)
TA	A formal notice issued by the DOD-CERT that does not require acknowledgment and compliance.
XO	Executive Officer.
Vulnerability	Weakness in an Information System, system security procedures, internal controls, or implementation that could be exploited. NSTISSI No. 4009 (Sep 2000)
VCTS	Vulnerability Compliance Tracking System. This is a DISA developed management tool used in tracking vulnerability notice compliance.

Annex B – Table of contents for VCTS online Users Guide.

1. INTRODUCTION
1.1. Purpose and Scope
1.2. Document Organization
1.3. Background
1.4. Process Overview with Flowchart
1.5. VCTS Help Desk
2. VCTS REQUIREMENTS
2.1. User Registration and Obtaining a System Userid
2.2. Web Browser Requirement
2.3. Email Requirement
3. VCTS GENERAL INFORMATION
3.1. Logon Procedures
3.2. VCTS NIPRNET Access (Unclassified)
3.3. VCTS SIPRNET Access (Classified)
3.4. VCTS Warning Page
4. VCTS HOME AND LINKS
4.1. Summary of the VCTS Home and Links
4.2. Screen Details of the VCTS Home and Links
4.3. Conditions of the VCTS Home and Links
5. REPORTS
5.1. Summary of Reports
5.2. Screen Details of Reports
5.3. IA06 - Receipt Acknowledgement by Program
5.4. IA07 - Program Action Plan Report
5.5. VS01 - Detailed Compliance Report by Status Categories
5.6. VS02 - Detailed Compliance Report by Actual Status
5.7. VS03 – Acknowledgement Status Report
5.8. VS04 - Extension Expiration Report
5.9. VS05 - Asset Permissions Report
5.10. VS06 – Organizational Structure Summary Report
5.11. VS07 - Extension History Report
5.12. VS08 – OS Vulnerability Summary Report
5.13. VS09 - Extension Status Report
5.14. VM01 - Compliance Summary Report by Organization
5.15. VM02 - Compliance Summary Report by Vulnerability
5.16. VM03 - Registered Users by Organization
5.16.1. Summary of Registered Users by Organization
5.17. VM04 - Registered Systems by Organization
5.18. VM07 - Compliance and Asset Information Extract
5.19. VM08 - Waiver Summary Report By Vulnerability
6. ASSET REGISTRATION
6.1. Summary of Asset Registration
6.2. VCTS Requests
7. ASSET PERMISSIONS

7.1. Summary of Asset Permissions
7.2. Screen Details of Asset Permissions
7.3. Conditions of Asset Permissions
8. ASSET STATUS
8.1. Summary of Asset Status
8.2. Screen Details of Asset Status
8.3. Conditions of Asset Status
9. RECEIPT ACKNOWLEDGEMENT
9.1. Summary of Receipt Acknowledgement
9.2. Screen Details of Receipt Acknowledgement
9.3. Conditions of Receipt Acknowledgement
10. PM RECEIPT ACKNOWLEDGEMENT
10.1. Summary of PM Receipt Acknowledgement
10.2. Screen Details of PM Receipt Acknowledgement
10.3. Conditions of Receipt Acknowledgement - Program Manager
11. C/S/A RECEIPT ACKNOWLEDGEMENT
11.1. Summary of C/S/A Receipt Acknowledgement
11.2. Screen Details of Receipt Acknowledgement - C/S/A POC / DOD Oversight
11.3. Conditions of Receipt Acknowledgement - C/S/A POC / DOD Oversight
12. PM ACTION PLAN
12.1. PM Extension Process
12.2. Summary of PM Action Plan
12.3. Screen Details of PM Action Plan
12.4. Conditions of PM Action Plan
13. EXTENSION ANALYSIS
13.1. Extension Analysis Process
13.2. Summary of Extension Analysis
13.3. Screen Details of Extension Analysis
13.4. Conditions of Extension Analysis
14. AUTOMATED STATUS UPDATE
14.1. Summary of Automated Status Update
14.2. Screen Details of Automated Status Update
14.3. Conditions of Automated Status Update
15. USER PERMISSIONS
15.1. Summary of User Permissions
15.2. Screen Details of User Permissions
15.3. Conditions of User Permissions
16. ORGANIZATIONAL CHART
16.1. Summary of Organizational Chart
16.2. ORGANIZATION DETAILS
16.3. Conditions of Organizational Chart and Details
17. UPDATE YOUR USER AND EMAIL INFO
17.1. Summary of Update Your User and Email Info
17.2. Screen Details of Update Your User and Email Info
17.3. Conditions of Update Your User and Email Info
18. CHANGE PASSWORD
18.1. Summary of Change Password

19. VCTS HELP
19.1. Summary of VCTS Help
20. APPENDIX A
20.1. Glossary
21. APPENDIX B
21.1. System Authorization Access Request (SAAR) - DISA Form 41
22. APPENDIX C
22.1. Points of Contact

Annex C – Sample VCTS IAVA Alert Message

The following is a sample notification message sent out as part of VCTS informing a user of a vulnerability notice.

Subject: Information Assurance Vulnerability Alert (IAVA) 1999-0003

1. The Defense Information Systems Agency (DISA) is releasing VULNERABILITY NOTICE 1999-0003 in accordance with the DISA IAVA Handbook located at URL https://datahouse.disa.mil/cio/IAVA /IAVA handbook.html.

2. At least one SA for each registered system potentially affected by this bulletin is required to acknowledge receipt with 5 days through the Vulnerability Compliance Tracking System (VCTS). In addition, all SAs are required to bring into compliance, request an extension, or indicate the bulletin is not applicable to the system. This status must be reported to the VCTS within 30 days. For unclassified systems, the URL is https://vcts.disa.mil. For classified systems (Secret and Confidential), the URL is https://vcts.disa.smil.mil.

3. If you are having difficulty accessing or using the application, please contact the RSA Chambersburg Helpdesk by telephone, 717-267-5690, DSN 570-5690 or 1-800-582-4764 or via NIPRNet email at weblog@chamb.disa.mil. If you have questions about the VCTS application, please email them to vms@chamb.disa.mil.

4. If you have questions regarding the IAVA process, please contact the CIO's office at 703-681-2558 or DSN 761-2558.

5. For further information about the IAVA bulletin itself, please contact the DOD-CERT Hotline at 703-607-4700, DSN 327- 4700, or 1-800-357-4231; or via NIPRNet email at cert@cert.mil. Information pertaining directly to this vulnerability will be posted on the ASSIST web site at http://www.cert.mil. A link to the DOD-CERT web site from the VCTS is also available.

Annex D – General Questions and Answers

What's defined in the VCTS? The VCTS was developed to track all information technology assets that can be affected by any issued alert. This includes systems, both developmental and operational, which are to be certified and accredited by each DAA. Assets that comprise each system will be populated and maintained by each SA or process identified by the activity ISSM. Assets that comprise each network will be populated and maintained by each SA or ISSM. The type of entries in the VCTS may increase as the IAVA process matures.

Extension – How is it used? An extension in the IAVA process has two uses. First, the extension can be used in the traditional sense where the DAA accepts the mitigated risk associated with nonstandard official corrective action. Second, the extension can be employed by the user to request additional time to allow for corrective action to occur.

Extension Request - Who requests an extension? The SA or ISSO submits an extension request. In the current version, the extension request is sent directly to the DAA for analysis and decision.

Extension Adjudication - Who decides if an extension is granted? The DAA, makes extension decisions for the IAVA process.

Open Status – What does it mean? When is "open" acceptable but not recommended? As soon as an asset is entered into the VCTS it has an "open" status, until a decision is made otherwise by the individual who has custody for the asset or by a program manager. "Open" means the asset is impacted by a specific alert, however, no protective actions have been put in place – so the vulnerability still exists. Most alerts are issued with a period of 30 days for compliance. An "open" status is acceptable during this 30-day period. However, if an asset becomes operational and is registered in the VCTS 30 days after the initial release of the alert, an "open" status is not acceptable.

Annex E – Fix Action Plan Format

Activity / Program	Status	# of Assets	Reason For Not Being Fixed	Action Plan	Estimated Fix Date
IAVA 2002-A-00#	Awaiting DAA approval	56	Testing and evaluation patch.	Assuming patch passes testing, will implement 6/11 – 7/10.	7/10/03
Managed Programs					
DISA Activity (i.e. CD, OPS, NS, etc.)					

Note:

Each activity ISSM must submit a consolidated activity Fix Action Plan to CIO the 7 days prior to IAVA compliance date or extension expiration.

All Fix Action Plans must be approved by the activity Deputy Director (DD).